IN THE CLAIMS

Please amend the claims as follows, a markup copy follows this clean copy as required under 37 CFR 1.121:

CLEAN COPY

53. (Once Amended) A computer readable medium containing program instructions for a software toolkit containing a collection of data structures and subroutines for developing an application for playing digital content data, the program instructions comprising instructions for:

01

receiving previously encrypted content data encrypted with an encryption key from an external source;

decrypting the received previously encrypted content data;

reencrypting the decrypted received content data with a local encrypting key wherein the local encrypting key is a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content;

storing the previously encrypted content data in a library;

selecting one or more encrypted content data from the library to play; and

decrypting each content data selected to be played with its unique decryption key,

wherein the decrypting is performed in a tamper-resistant subroutine for deterring unauthorized access to the instructions for decrypting the content data and for deterring unauthorized access to the decryption key; and;

wherein the decrypting and reencrypting instructions are performed in the tamper resistance subroutine.

54. (Once Amended) The computer readable medium according to claim 53, wherein the step of reencrypting the decrypted received content data with a local encrypting key includes encrypting with IBM's SEAL algorithm.

Trade mark
217 3.05 (u)
6 08.01

01

55. (Once amended) The computer readable medium according to claim 53, wherein the instruction for reencrypting the decrypted received content data utilizes a unique local decrypting key for each content data prior to storage in the library.

73. (Once Amended) A method for providing a collection of data structures and subroutines for developing an application for playing digital content data, the method comprising the steps of:

receiving previously encrypted content data encrypted with an encrypted key from an external source;

02

decrypting the received previously encrypted content data;

reencrypting the decrypted received content data with a local encrypting key wherein the local encrypting key is a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content;

storing the previously encrypted content data in a library;

selecting one or more encrypted content data from the library to play; and

decrypting each content data selected to be played with its unique decrypting key;

wherein the decrypting is performed in a tamper-resistant subroutine for deterring unauthorized access to the instructions for decrypting the content data and for deterring unauthorized access to the decrypting key; and

wherein the decrypting and reencrypting instructions are performed in the tamper resistance subroutine.

74. (Once Amended) The method according to claim 73, further comprising the step of:

decrypting the received previously encrypted content data prior to storage in the library;

reencrypting the decrypted received content data with a local encrypting key includes encrypting with IBM's SEAL algorithm.

02

75. (Once Amended) The method according to claim 74, wherein the step for reencrypting the decrypted received content data utilizes a unique local decrypting key for each content data prior to storage in the library.

83. (New) An end user device for rendering encrypted content comprising:

an interface to a computer readable medium for receiving previously encrypted content data encrypted with an encrypted with a key from an external source;

an interface to a library for storage of the content;

a software application for

03

decrypting the received previously encrypted content;

reencrypting the decrypted received content data with a local encrypting key wherein the local encrypting key is a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content; and

storing the previously encrypted content data in the library;

a user interface for selecting one or more encrypted content data from the library to play; and

a tamper resistant environment which deterring unauthorized access to the instructions for decrypting the content data and for deterring unauthorized access to the decrypting key, whereby inside the tamper resistant environment each content data selected to be played is decrypted with its unique decrypting key; and

wherein the decrypting and reencrypting instructions are performed in the tamper resistance environment.

84. (New) The end user device according to claim 83, wherein the local encrypting key includes IBM's SEAL algorithm.

85. (New) The end user device according to claim 83, wherein the local encrypting key includes a unique local encryption key for each content data prior to storage in the library.

86. (New) The end user device according to claim 85, wherein the software application stores the unique local encryption key in several distinct parts throughout an information processing system.

03

87. (New) The end user device according to claim 84, wherein the software application stores the common local encryption key in several distinct parts throughout an information processing system.